SYSTEM, METHOD AND APPARATUS FOR PROVIDING MULTIPLE ACCESS MODES IN A DATA COMMUNICATIONS NETWORK

Inventor: Philip Kwan

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention is generally directed to data communications networks. In particular, the present invention is directed to providing multiple access modes in a data communications network.

Background

[0002] There is an increasing demand for flexible security features for controlling access to data communications networks. This is due, in large part, to an increase in the use of a wide variety of portable computing and communication devices such as laptop computers and Voice Over Internet Protocol (VOIP) telephones. These devices, which often use different protocols for access and security, can be easily moved from one network access point to another, or from one network to another network. While such mobility and ease of access may be desirable from an end user perspective, it creates significant concerns from the perspective of network access and security.

[0003] For wired networks, recent security solutions from network vendors have involved pushing authentication and access functions out to the layer 2 port, such as to a layer 2 switch. Typical solutions involve user authentication at the layer 2 switch in accordance with protocols defined by, for example, the IEEE 802.1x standard. However, at present, only a small percentage of portable computing devices provide 802.1x support (i.e., have embedded 802.1x client software). When a user device does not support the user authentication protocol, conventional layer 2 switches drop the offending device, and deny access to the network. In other words, conventional switches employ a binary protocol as a first step, wherein access depends on whether the user device supports a particular user authentication protocol, such as a user authentication protocol in accordance with the IEEE 802.1x standard.

[0004] This conventional method of authentication and access limits the flexibility of conventional layer 2 switches. For example, in a common enterprise scenario, a visitor to an organization attends a meeting in a conference room that is fully wired for access to the organization's local area network (LAN). A sophisticated user authentication protocol, such as a user authentication protocol in accordance with the IEEE 802.1x standard, allows authorized users access to one or more virtual local area networks (VLANs). However, if the visitor's laptop computer does not support the user authentication protocol, then conventional layer 2 switches will deny all access to the organization's LAN. As a result, the visitor would not be able to perform such basic functions as checking e-mail on the Internet, placing or receiving a VoIP telephone call, or availing herself of other online functions that would not otherwise compromise organizational security.

[0005] What is needed then is an access solution that improves upon and addresses the shortcomings of known access and authentication solutions.

BRIEF SUMMARY OF THE INVENTION

[0006] The present invention is directed to a network access system, method and apparatus that substantially obviates one or more of the problems and disadvantages of the related art.

[0007] In particular, the present invention is directed to a network access device, such as a network switch, that provides at least one additional access mode for user devices that do not support a user authentication protocol used by a host network. For example, an embodiment of the present invention grants limited access to a user device even if the user device does not support a user authentication protocol recognized by the host network, such as a protocol in accordance with the IEEE 802.1x standard. Such flexibility allows a visitor to an organization access to a pre-configured low-security VLAN, or one of a plurality of pre-configured low-security VLANs depending on the type of user device, even if the user device does not support the authentication protocol used by the host network.

[0008] The present invention is an advance over conventional network switches that implement the 802.1x user authentication protocol. Such conventional switches place a user device in either one of two states: an authorized state, in which full network access is permitted, or an unauthorized state, in which network access is denied and the only packets that may be received from the user device are 802.1x control packets. Thus, a user device that does not include an 802.1x client will be denied all network access by such switches. An embodiment of the present invention addresses this problem by providing at least a third authorization state, which may be thought of as "semi-authorized," in which some form of limited network access is allowed.

[0009] In accordance with one embodiment of the present invention, a method for providing multiple access modes in a data communications network is disclosed. The method includes sensing a user device coupled to a port of a network access device, determining if the user device supports a user authentication protocol used by a host network, and placing the port into a semi-authorized access state if it is determined that the user device does not support the user authentication protocol. The semi-authorized access state then limits access by the user device to a pre-configured network accessible via the data communications network.

[0010] In an alternate embodiment of the present invention, a network access device for providing multiple access modes is provided. The network access device comprises a plurality of input ports, a plurality of output ports, a switching fabric for routing data received on the plurality of input ports to at least one of the plurality of output ports, and control logic. The control logic is adapted to determine whether a user device coupled to one of the plurality of input ports supports an authentication protocol used by a host network, and to place the input port into a semi-authorized access state if the authentication protocol is not supported, thereby providing the user device with limited access to a pre-configured network accessible via the host network.

[0011] Further features and advantages of the invention, as well as the structure and operation of various embodiments of the invention, are described in detail below with reference to the accompanying drawings. It is noted that the invention is not limited to the specific embodiments described herein. Such embodiments are presented herein for illustrative purposes only. Additional embodiments will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein.

BRIEF DESCRIPTION OF THE DRAWINGS/FIGURES

[0012] The accompanying drawings, which are incorporated herein and form part of the specification, illustrate the present invention and, together with the description, further serve to explain the principles of the invention and to enable a person skilled in the relevant art(s) to make and use the invention.

[0013] FIG. 1 depicts the basic elements of a data communications network that provides multiple network access modes in accordance with an embodiment of the present invention.

[0014] FIG. 2 depicts an exemplary high-level architecture of a network access device, such as a network switch, in accordance with an embodiment of the present invention.

[0015] FIG. 3 is a flowchart of a method for providing multiple access modes in a data communications network in accordance with an embodiment of the present invention.

[0016] FIG. 4 is a flowchart of an alternate method for providing multiple access modes in a data communications network in accordance with an embodiment of the present invention.

[0017] FIGs. 5A and 5B depict a flowchart of a method for providing additional levels of security in a data communications network that provides multiple access modes in accordance with an embodiment of the present invention.

[0018] FIG. 6 is a flowchart of a method for enabling physical address authentication as described in reference to FIG. 5A.

[0019] FIG. 7 depicts a data communications network that provides multiple access modes and accommodates a plurality of user devices in a multi-host configuration in accordance with an embodiment of the present invention.

[0020] The features and advantages of the present invention will become more apparent from the detailed description set forth below when taken in conjunction with the drawings, in which like reference characters identify corresponding elements throughout. In the drawings, like reference numbers generally indicate identical, functionally similar, and/or structurally similar elements. The drawings in which an element first appears is indicated by the leftmost digit(s) in the corresponding reference number.

DETAILED DESCRIPTION OF THE INVENTION

A. Overview

[0021] The present invention is directed to a system, method and apparatus for providing multiple access modes in a data communications network. The system, method and apparatus provides at least three levels of network access. The particular level of access depends on whether a user device is configured to support an authentication protocol used by the host network. In conventional network access devices, the inability to communicate with the host network using a particular user authentication protocol, such as the IEEE 802.1x protocol, results in a denial of access to subsequent levels of authentication, and termination of the network connection.

[0022] In an embodiment of the present invention, a network access device is configured to provide one or more default access modes. A user device coupled to a port of the network access device can be automatically limited to one of the one or more pre-configured access modes if the user device does not support an authentication protocol used by the host network. The pre-configured access mode may limit access to, for example, a Voice over Internet Protocol (VoIP) network, the Internet, or a pre-configured virtual local area network (VLAN).

B. System, Method and Apparatus for Providing Multiple Access Modes in Accordance with an Embodiment of the Present Invention

[0023] FIG. 1 depicts the basic elements of data communications network 100 that provides multiple network access modes in accordance with an embodiment of the present invention. As shown in FIG. 1, data communications network 100 comprises a host network 104, a network access device 102 and an authentication server 106 each of which is communicatively coupled to host network 104, and a user device 108 that is communicatively coupled to network access device 102.

[0024] Host network 104 comprises a plurality of network nodes interconnected via a wired and/or wireless medium, wherein each node consists of a device capable of transmitting or receiving data over host network 104. In the embodiment described herein, host network 104 comprises a conventional local area network (LAN) that employs an Ethernet communication protocol in accordance with the IEEE 802.3 standard for data link and physical layer functions. However, the invention is not so limited, and host network 104 may comprise other types of networks, including but not limited to a wide area network (WAN), and may employ other types of communication protocols, including but not limited to ATM, token ring, ARCNET, or FDDI (Fiber Distributed Data Interface) protocols.

[0025] As shown in FIG. 1, host network 104 is communicatively coupled to a plurality of external networks, or "extranets," including the Internet 110 and a Voice over Internet Protocol (VoIP) network 112. As will be appreciated by persons skilled in the relevant art(s), access to the extranets is facilitated by one or more network gateway devices, which comprise part of host network 104.

[0026] Network access device 102, which preferably comprises a network switch, is a device that comprises a plurality of ports for communicatively interconnecting network devices to each other and to host network 104. Network access device 102 is configured to channel data units, such as data packets or frames, between any two devices that are attached to it up to its maximum number of ports. In terms of the International Standards Organization's Open Systems Interconnection (OSI) model, network access device 102 performs layer 2, or data link layer, functions. In particular, network access device 102 examines each received data unit and, based on a destination address included therein, determines which network device the data unit is intended for and switches it out toward that device. In the embodiment described herein, the destination address comprises a physical or Media Access Control (MAC) address of a destination device.

[0027] FIG. 2 depicts an exemplary high-level architecture of network access device 102 in accordance with an embodiment of the present invention. As shown in FIG 2, network access device 102 comprises a plurality of input ports, 204a through 204n, that are coupled to a plurality of output ports, 206a through 206n, via a switching fabric 202. The designation of ports as either input ports or output ports is arbitrary as one skilled in the art would recognize that ports facilitate data transmission in either direction. Network access device 102 also includes control logic 208 for controlling various aspects of network access device operation and a user interface 210 to facilitate communication with control logic 208. User interface 210 provides a means for a user, such as a system administrator, to reconfigure network access device 102 and adjust operating parameters.

[0028] In operation, data units (e.g, packets or frames) are received and optionally buffered on one or more of input ports 204a through 204n. Control logic 208 schedules the serving of data units received by input ports 204a through 204n in accordance with a predetermined scheduling algorithm. Data units are then served to switching fabric 202, which routes them to the appropriate output port 206a through 206n based on, for example, the destination address of the data unit.

[0029] Output ports 206a through 206n receive and optionally buffer data units from switching fabric 202, and then transmit them on to a destination device. In accordance with an embodiment of the present invention, network access device 102 may also include logic for performing routing functions (layer 3 or network layer functions in OSI).

[0030] With further reference to FIG. 1, user device 108 is shown connected to one of the ports of network access device 102. User device 108 may comprise a personal computer (PC), laptop computer, Voice Over Internet Protocol (VOIP) phone, or any other device capable of transmitting or receiving data over a data communications network, such as network 100.

[0031] Authentication server 106 comprises a computer that stores application software and a database of profile information for performing a user authentication protocol that will be described in more detail herein. In an embodiment, authentication server 106 comprises a server that uses the Remote Authentication Dial-In User Service (RADIUS) as set forth in Internet Engineering Task Force (IETF) Request For Comments (RFC) 2865 for performing user authentication functions.

[0032] FIG. 3 illustrates a flowchart 300 of a method for providing multiple access modes in a data communications network in accordance with an embodiment of the present invention. The invention, however, is not limited to the description provided by the flowchart 300. Rather, it will be apparent to persons skilled in the relevant art(s) from the teachings provided herein that other functional flows are within the scope and spirit of the present invention. Flowchart 300 will be described with continued reference to data communications network 100 and network access device 102 described above in reference to FIGS. 1 and 2. The invention, however, is not limited to those embodiments.

[0033] The method of flowchart 300 begins at step 301, in which one of the input ports 204a-204n (referred to hereinafter as input port 204) is configured to provide a default-public access mode for devices that do not support a user authentication protocol used by host network 104. In an embodiment, the default-public access mode is a semi-authorized access state that limits network access to Internet 110, VoIP network 112, or another low-security VLAN that is outside the organization's secure LAN. The specific type of semi-authorized access state provided to a user device 108 not supporting the user authentication protocol used by host network 104 can be configured by a network administrator via user interface 210.

[0034] In step 305, user device 108 is sensed at input port 204 of network access device 102. Control logic 208 senses user device 108 when it is coupled to input port 204. Coupling user device 108 to input port 204 may comprise, for example, coupling user device 108 to an RJ-45 connector, which is in turn wired to input port 204.

[0035] At step 310, network access device 102 determines whether user device 108 supports a user authentication protocol used by host network 104. To accomplish this, control logic 208 polls user device 108 for a user authentication protocol. In an embodiment, the user authentication protocol is IEEE 802.1x.

[0036] At step 315, control logic 208 performs one of two actions. If user device 108 does not support the user authentication protocol, control logic 208 places network access device port 204 in a semi-authorized access state, as shown at step 320. If user device 108 does support the user authentication protocol, control logic 208 begins further authentication in accordance with the user authentication protocol, as shown at step 365.

[0037] Where the user authentication protocol is IEEE 802.1x, these steps are carried out as will now be described. Network access device 102 forces the user's client software into an unauthorized state that allows the client to send only an extensible authentication protocol (EAP) start message. If user device 108 supports IEEE 802.1x, then step 365 is invoked, and the authentication procedure begins in accordance with IEEE 802.1x. Accordingly, network access device 102 transmits an EAP message requesting the user's identity (e.g., a user name and password). The client returns the identity, which is then forwarded by network access device 102 to authentication server 106, which uses an algorithm to authenticate the user and then returns an accept or reject message back to network access device 102. Assuming an accept message was received, network access device 102 changes the client's state to authorized and normal communication can take place.

[0038] If user device 108 does not support IEEE 802.1x, as evidenced by lack of authentication attempts after N seconds, step 320 is invoked. In step 320, control logic 208 places input port 204 into a semi-authorized access state. As described above, in this embodiment, the semi-authorized access state causes the port to restrict access to Internet 110, VoIP network 112, or another low-security VLAN defined by the network administrator that is outside the organization's secure LAN.

[0039] In an alternative embodiment, not shown in FIG. 3, port 204 is configured to additionally provide a default-secure access mode. In a default-secure access mode, if user device 108 does not support a user authentication protocol used by host network 104, then the entire port 204 is blocked and secured. This option is available for installations that do not desire to provide guests access to the Internet or other semi-authorized networks.

C. System, Method and Apparatus for Providing Multiple Access Modes Based on User Device Type in Accordance with an Embodiment of the Present Invention

[0040] FIG. 4 illustrates a flowchart 400 of an alternate method for providing multiple access modes in a data communications network in accordance with an embodiment of the present invention. In particular, flowchart 400 describes an embodiment of the present invention wherein the default-public access mode comprises a plurality of pre-configured semi-authorized access states. Each of these states provide limited network access to a corresponding one of a plurality of low security VLANs as configured by a network administrator. If user device 108 does not support a user authentication protocol used by host network 104, the input port to which user device 108 is coupled is selectively placed into one of the plurality of pre-configured semi-authorized access states depending on the type of user device 108 (e.g., VoIP telephone or portable computing device). The invention, however, is not limited to the description provided by flowchart 400. Rather, it will be apparent to persons skilled in the relevant art(s) from the teachings provided herein that other functional flows are within the scope and spirit of the present invention. Flowchart 400 will also be described with continued reference to data communications network 100 and network access device 102 described above in reference to FIGS. 1 and 2. The invention, however, is not limited to those embodiments.

[0041] The method of flowchart 400 begins at step 401, in which one of input ports 204a-204n of network access device 102 (referred to hereinafter as input port 204) is configured to provide a default-public access mode. In this embodiment, the default-public access mode comprises at least two semi-authorized access states. This is in contrast to step 301 of FIG. 3, in which the default-public access mode comprises only one semi-authorized access state. For example, in the present embodiment, input port 204a can be configured to allow network access only to the Internet or a VoIP network depending on the type of user device coupled to the port. Similarly, a second input port 204b can be configured to allow network access only to the Internet, a VoIP network, or some other low security VLAN depending on the type of user device coupled to the port. One skilled in the art can envision various desirable combinations based on, for example, the location of the input port.

[0042] In step 405, user device 108 is sensed at input port 204 of network access device 102 in a manner similar to that described above in reference to step 305 of flowchart 300. Control logic 208 senses user device 108 when it is coupled to input port 204. Coupling user device 108 to input port 204 may comprise, for example, coupling user device 108 to an RJ-45 connector, which is in turn wired to input port 204.

[0043] In step 410, network access device 102 determines whether user device 108 supports a user authentication protocol used by host network 104 in a manner similar to that described above in reference to step 310 of flowchart 300. To accomplish this, control logic 208 polls user device 108 for a user authentication protocol. In an embodiment, the authentication protocol is IEEE 802.1x.

[0044] In step 415, control logic 208 performs one of two actions. If user device 108 does not support the user authentication protocol, the method proceeds to determining the type of user device that has been sensed at input port 204, as shown in step 417. To determine the type of user device 108, user device 108 is polled by control logic 208A variety of known techniques for distinguishing between various types of user devices are readily available to persons skilled in the relevant art(s). As shown at step 420, control logic 208 then selectively places input port 204 into one of the at least two semi-authorized access states configured in step 401 based on the type of user device. For instance, if user device 108 is a VoIP telephone, then input port 204 will default to a semi-authorized state that includes a VoIP network, and thus provide user device 108 with restricted access to VoIP network 112. Likewise, if user device 108 is a laptop computer, then input port 204 will default to a semi-authorized state that includes the Internet, and thus provide user device 108 with restricted access to the Internet 110. These examples are not meant to be limiting. One skilled in the art can envision a variety of pre-configured low security networks to which a user device 108 can be provided access based on device type in accordance with this embodiment of the present invention.

[0045] If user device 108 does support the user authentication protocol, control logic 208 begins further authentication in accordance with the user authentication protocol, as shown at step 465.

D. Method for Providing Additional Levels of Security in a Data Communications Network that Provides Multiple Access Modes in Accordance with an Embodiment of the Present Invention

[0046] FIGS. 5A and 5B depict flowcharts 500A and 500B of a method for providing additional levels of security in a data communications network that provides multiple access modes in accordance with the present invention. The additional levels of security may comprise validation of a media access control (MAC) address, or physical address, of a user device coupled to a port of a network access device, as well as dynamic VLAN assignment of the user device. The invention, however, is not limited to the description provided by flowcharts 500A and 500B. Rather, it will be apparent to persons skilled in the relevant art(s) from the teachings provided herein that other functional flows are within the scope and spirit of the present invention. Flowcharts 500A and 500B will also be described with continued reference to data communications network 100 and network access device 102 described above in reference to FIGS. 1 and 2. The invention, however, is not limited to those embodiments.

[0047] The method of flowcharts 500A and 500B begins at step 501 in which one of input ports 204a-204n of network access device 102 (referred to hereinafter as input port 204) is configured to provide a default-public access mode. This step is further described above in relation to step 301 of flowchart 300.

[0048] At step 505, a user device 108 is sensed at input port 204 of network access device 102, as further described above in reference to step 305 of flowchart 300. At step 507, network access device 102 authenticates a physical (MAC) address of user device 108. Network access device 102 performs this step by comparing a MAC address of user device 108 with a limited number of "secure" MAC addresses that are stored by network access device 102.

[0049] As shown at step 509, if packets received from user device 108 have a source MAC address that does not match any of the secure addresses, then there is a security violation and the protocol proceeds to step 555, in which network access device 102 either drops the packets or alternately, disables input port 204 entirely. Thus, a first additional layer of security is provided in which a physical (MAC) address is validated before user device 108 is allowed any access to host network 104. This feature is described in more detail in Section E, below.

[0050] However, as also shown at step 509, if packets received from user device 108 have a source MAC address that does match one of the secure addresses, then no security violation has occurred, and the protocol proceeds to step 510, in which network access device 102 determines whether user device 108 supports a user authentication protocol used by host network 104. This step is more fully described above in reference to step 310 of flowchart 300.

[0051] At step 515, control logic 208 performs one of two actions in a manner similar to that described above in reference to step 315 of flowchart 300. If user device 108 does not support the user authentication protocol, control logic 208 places network access device port 204 in a semi-authorized access state, as shown at step 520. If user device 108 does support the user authentication protocol, control logic 208 begins further authentication in accordance with the user authentication protocol, as shown at step 565.

[0052] FIG. 5B depicts a continuation of the authentication procedure that was begun in step 565 of FIG. 5A, and provides an additional level of security for user devices 108 that do support a recognizable authentication protocol. This additional level of security may be referred to as dynamic VLAN assignment. In an embodiment in which the user authentication protocol is IEEE 802.1x, dynamic VLAN provisioning is carried out as will now be described.

[0053] At step 570, network access device 102 authenticates a user of user device 108 based upon credentials provided by the user. In accordance with 802.1x, this entails sending the user credentials in a request message to authentication server 106 and receiving an accept or reject message in return, the accept or reject message indicating whether the user is valid. As shown at step 572, if the user is not valid, then the security protocol proceeds to step 574, in which control logic 208 places input port 204 in a semi-authorized state. However, as also shown at step 572, if the user is valid, then the security protocol proceeds to step 576.

[0054] At step 576, network access device 102 determines whether or not the user is associated with a VLAN supported by network access device 102. In an embodiment, this step entails determining whether a VLAN identifier (ID) or a VLAN Name was returned as part of the accept message from authentication server 106. If the user is not associated with a VLAN supported by network access device 102, control logic 208 places input port 204 in a semi-authorized state. If, however, the user is associated with a VLAN supported by network access device 102, then network access device 102 assigns the port to the specified VLAN and begins processing packets from user device 108, as shown at step 580.

[0055] With reference to the exemplary switch embodiment of FIG. 2, the access functions performed by network access device 102, as described above, are performed by control logic 208. As will be appreciated by persons skilled in the art, such functions may be implemented in hardware, software or a combination thereof.

[0056] Further details regarding the performance of physical (MAC) address device validation and dynamic VLAN assignment in a network access device are provided in commonly-owned, co-pending U.S. Patent Application No. (*to be assigned; Atty. Docket No. 1988.0170000*), entitled "Multiple Tiered Network Security System, Method and Apparatus" to Kwan *et al.*, filed June 11, 2003, the entirety of which is incorporated by reference as if set forth fully herein.

E. Physical Address Authentication of User Device in Accordance with an Embodiment of the Present Invention

[0057] As discussed above, in accordance with an embodiment of the present invention, network access device 102 is adapted to perform a physical (MAC) address authentication of a user device that is coupled to one of its ports. In particular, network access device 102 is adapted to store a limited number of "secure" MAC addresses for each port. A port will forward only packets with source MAC addresses that match its secure addresses. In an embodiment, the secure MAC addresses are specified manually by a system administrator via user interface 210. In an alternate embodiment, network access device 102 learns the secure MAC addresses automatically. If a port receives a packet having a source MAC address that is different from any of the secure learned addresses, a security violation occurs.

[0058] With reference to the embodiment of network access device 102 depicted in FIG. 2, secure addresses for each input port 204a through 204n are stored in a local memory assigned to each port. Alternately, secure addresses are stored in a shared global memory, or in a combination of local and global memory (not shown).

[0059] In an embodiment, when a security violation occurs, network access device 102 generates an entry to a system log and an SNMP (Simple Network Management Protocol) trap. In addition, network access device 102 takes one of two actions as configured by a system administrator: it either drops packets from the violating address or disables the port altogether for a specified amount of time.

[0060] In a further embodiment of the present invention, a system administrator can configure network access device 102 to re-direct packets received from the violating address to a different network destination than that originally intended. Network access device 102 may achieve this by altering the packet headers. For example, network access device 102 may alter a destination address of the packet headers. Alternately, the re-direction may be achieved by generating new packets with identical data payloads but having different packet headers. As will be appreciated by persons skilled in the relevant art(s), the decision to configure network access device 102 to re-direct traffic from a violating address may be premised on the resulting burden to network access device 102 in handling traffic.

[0061] FIG. 6 illustrates a flowchart 600 of a method for enabling physical address authentication of a device coupled to a data communications network in accordance with an embodiment of the present invention. In particular, flowchart 600 represents steps performed by a system administrator in order to configure a network access device to perform physical address authentication as described above in reference to step 507 of FIG. 5A. The invention, however, is not limited to the description provided by the flowchart 600. Rather, it will be apparent to persons skilled in the relevant art(s) from the teachings provided herein that other functional flows are within the scope and spirit of the present invention.

[0062] At step 602, the system administrator enables the MAC address authentication feature for one or more ports of the network access device. In an embodiment, the security feature is disabled on all ports by default, and a system administrator can enable or disable the feature globally on all ports at once or on individual ports.

[0063] At step 604, the system administrator sets a maximum number of secure MAC addresses for a port. In an embodiment, the network access device utilizes a concept of local and global "resources" to determine how many MAC addresses can be secured on each port. In this context, "resource" refers to the ability to store one secure MAC address entry. For example, each interface may be allocated 64 local resources and additional global resources may be shared among all the interfaces on the network access device.

[0064] In an embodiment, when the MAC address authentication feature is enabled for a port, the port can store one secure MAC address by default. A system administrator can then increase the number of MAC addresses that can be secured to a maximum of 64, plus the total number of global resources available. The number of addresses can be set to a number from 0 to (64 + the total number of global resources available). For example, the total number of global resources may be 2048 or 4096, depending on the size of the memory allocated. When a port has secured enough MAC addresses to reach its limit for local resources, it can secure additional MAC addresses by using global resources. Global resources are shared among all the ports on a first come, first-served basis.

[0065] At step 606, the system administrator sets an age timer for the MAC address authentication feature. In an embodiment, secure MAC addresses are not flushed when a port is disabled and brought up again. Rather, based on how the network access device is configured by the system administrator, the secure addresses can be kept secure permanently, or can be configured to age out, at which time they are no longer secure. For example, in an embodiment, the stored MAC addresses stay secure indefinitely by default, and the system administrator can optionally configure the device to age out secure MAC addresses after a specified amount of time.

[0066] At step 608, the system administrator specifies secure MAC addresses for a port. Alternately, the network access device can be configured to automatically "learn" secure MAC addresses by storing the MAC addresses of devices coupled to the port up to the maximum number of secure addresses for the port. These stored MAC addresses are then used as the secure addresses for authentication purposes.

[0067] At step 610, the system administrator optionally configures the switch to automatically save the list of secure MAC addresses to a startup-configuration ("startup-config") file at specified intervals, thus allowing addresses to be kept secure across system restarts. For example, learned secure MAC addresses can be automatically saved every twenty minutes. The startup-config file is stored in network access device memory (not shown). In an embodiment, by default, secure MAC addresses are not automatically saved to a startup-config file.

[0068] At step 612, the system administrator specifies the action taken when a security violation occurs. In the case where the system administrator has specified the secure MAC addresses for the port, a security violation occurs when the port receives a packet with a source MAC address that is different than any of the secure MAC addresses. In the case where the port is configured to "learn" secure MAC addresses, a security violation occurs when the maximum number of secure MAC addresses has already been reached, and the port receives a packet with a source MAC address that is different than any of the secure MAC addresses. In an embodiment, the system administrator configures the network access device to take one of two actions when a security violation occurs: either drop packets from the violating address or disable the port altogether for a specified amount of time. This is illustrated in step 555 of flowchart 500 depicted in FIG. 5.

F. Multiple Access Mode System, Method and Apparatus for Multi-Host Environments in Accordance with an Embodiment of the Present Invention

[0069] The multiple access mode protocols and methods described above may be advantageously implemented in both single host and multiple host (multi-host) environments. FIG. 1 depicts a single host environment, as only a single user device 108 is coupled to a port of network access device 102. FIG. 7 depicts an alternate embodiment of the present invention that accommodates a plurality of user devices 108a-108n in a multi-host configuration. In particular, system 700 of FIG. 7 comprises a host network 104, which is communicatively coupled to a network access device 102, and an authentication server 106. A central user device 704 is coupled to network access device 102 and a plurality of additional user devices 108a through 108n are coupled to network access device 102 via central user device 704 in a multi-host configuration.

[0070] The multiple access mode methods described above may be advantageously implemented in system 700 in a variety of ways. For example, network access device 102 may perform physical (MAC) address authentication of central user device 704 only, and then authenticate the users of all the user devices if it determines that central user device 704 has a valid MAC address. If central user device 704 has an invalid MAC address, then the port may be closed to all user devices. Alternately, network access device 102 may perform physical (MAC) address validation of each of the user devices prior to authenticating their users. In this case, network access device 102 can selectively accept packets from user devices having valid MAC addresses while dropping packets from user devices having invalid MAC addresses.

[0071] In a similar fashion, network access device 102 can also selectively place user devices that do not support an authentication protocol used by the host network 104 in a semi-authorized access state as described above.

G. Conclusion

[0072] While various embodiments of the present invention have been described above, it should be understood that they have been presented by way of example only, and not limitation. It will be understood by those skilled in the relevant art(s) that various changes in form and details may be made therein without departing from the spirit and scope of the invention as defined in the appended claims. Accordingly, the breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.